Before the

FEDERAL COMMUNICAITONS COMMISSION

Washington, DC 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls - Reassigned Number	)	
NOI Advanced Methods to Target and	)	
Eliminate Unlawful Robocalls	)	
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

Table of Contents

REPLY COMMENTS OF RICHARD SHOCKEY

My name is Richard Shockey. I am the principal of Shockey Consulting located in Fairfax County Virginia. I am a member of the FCC North American Numbering Council [NANC]. I am also the Chairman of the Board of Directors of the SIP Forum, an industry promotion group for the Session Initiation Protocol [SIP] which is the principal technical standard for the Ongoing TDM to IP Evolution.[1] The SIP Forum is actively partnering with the Alliance for Telecommunications Industry Solutions [ATIS] on advanced Call Validation technologies and Call Validation Display techniques commonly known as STIR/SHAKEN that will complement the current discussion and may be the subject of further Commission actions in the future. [2][3]

That robocalls and spoofing are a problem needs no further discussion as the record in this Proceeding demonstrates. We are all aware that it is the #1 complaint to the Federal Communications Commission and the #1 Complaint to the Federal Trade Commission. It is also the #1 Complaint to the Canadian Radio-television and Telecommunications Commission and the #1 complaint to OFCOM the national regulator for communications in the United Kingdom. [4]

---

[1] Views contained in this document are purely those of Mr. Shockey and do not necessarily represent the views of the SIP Forum its member companies and participants. www.sipforum.org

[2] https://www.sipforum.org/activities/technical-wg-overview-and-charter/atissip-forum-nni-task-force-charter/

[3] https://www.sipforum.org/download/shaken-stired-thoughts-current-state-anti-spoofing-caller-validation-robocall-mitigation-call-validation-display/?wpdmdl=3365

[4] http://www.nanc-chair.org/docs/mtg_docs/Mar17_NANC_Robocall_Spoofing_Update.pdf

In general terms, we all know how this problem originated. The American People wanted competitive communications markets for voice communications. We now have them. No good deed goes unpunished. The Voice Communications industry is in the midst of a complicated transition from classic Circuit Switched, Time-Division Multiplexing and Signaling System 7 to all IP based SIP and IMS networks. The confluence of these two events created multiple vulnerabilities in the national voice communications system that have been exploited by criminal elements. The time has come to close these vulnerability's once and for all.

The current Notice of Proposed Rule Making and Notice of Inquiry should be viewed *a start* and *only the beginning,* to a rather long and complicated process of rebuilding trust in our national voice communications networks. The current NPRM/NOI focuses on several elements that will be useful in combating robocalls and spoofing but individually will not solve the problem. Nearly every commenter, including myself, has emphasized there is no "Silver Bullet". Commission and Industry efforts will end up being a series of "block and tackle" and "flanking maneuvers" that separately cannot address the problem but in combination will have a significant and long-lasting impact.

It is not necessary here to review the outstanding work done by the Industry led Strikeforce on Robocalls. [5] Those reports are an essential foundation for the multifaceted solution that is necessary to restore Trust, Security and Reliability in the Voice Networks of the United States.

The Role of Do Not Originate Databases

The current NPRM/NOI set focuses on two distinct issues. First is clarification of the rights and potentially obligation of service providers to block calls that are clearly spoofed. Second is the potential establishment of a National Do Not Originate [DNO] list of

---

[5] https://www.fcc.gov/ecfs/filing/10428413802365

Telephone Numbers that could be used to preemptively block calls deemed obviously spoofed.

I join the unanimous view of the Industry that the FCC should establish a Do Not Originate database. Reports from the Strikeforce indicate a high degree of success in blocking specific numbers used by the IRS and others in others in high profile fraud operations.

I support a reasoned policy of Safe Harbor for Telecommunications providers that act In Good Faith to attempt to eliminate robocalls and spoofing in their networks.

The NPRM/NOI seeks answers on what kinds of data should be included in a DNO database, how it should be distributed, and when it should be used by service providers at call origination. The principal issue at this point, is what data should be included. I specifically recommend that the data set for the DNO be as relatively static as possible and not require a more dynamic real time look up to external databases. The most obvious number sets for inclusion are the non-allocated parts of the North American Numbering Plan [NANP] for the US portions of the NANP and specific numbers such as IRS numbers, Department of Justice and PSAP numbers that have come under specific forms of attack in recent years. These sets should be relatively easy to collect. Service providers could down load these numbering data sets and periodic updates relatively easily and those numbers could be locally cached within the internal telephony service network infrastructure that carriers use to preform number translations and call routing. This is easily achievable within the current advanced SIP/IMS infrastructure that now completes nearly 50% of all landline calls in the US and with the ongoing deployment of Voice over LTE [VoLTE] will represent over 85% of all calls in the United States in the foreseeable future. In my judgement, the cost of implementing static DNO databases would not be burdensome on the industry.

I do not recommend inclusion of numbers allocated to service providers by the NANPA but not issued by service providers or disconnected, reassigned numbers *at this time*. It may be difficult to obtain this data from carrier internal carrier OSS/BSS systems and could include false positives. In addition, the disclosure of disconnected, reassigned and non-issued

numbers is extremely sensitive to service providers and may represent unwarranted disclosure of market data. It is important to note that as part of the Number Portability Administration Center [NPAC] contracts, the operator of the NPAC is specifically prohibited from any disclosure or marketing of number porting data. The unintended consequences of large scale disclosure of such data have not been carefully considered.

In addition, the disclosure of disconnected, reassigned or non-carrier issued numbers may run afoul of various aspects of the Commission's rules on Customer Proprietary Network Information [CPNI]. Think about it. Do you want people to know you have changed numbers or service providers? Do you want people to know you have moved? I urge extreme caution when considering including these data sets. Tracing name and address to phone numbers is a relatively simple process.

IMHO the addition of disconnected, reassigned or non-allocated numbers into the DNO system would require the establishment of a much more expansive DNO database with virtually real-time capabilities. That could increase cost to the industry without any demonstrable benefit to consumers. I have no basis to estimate the cost of such a real-time database to the industry but if our experience with Local Number Portability is any guide the cost could range in the hundreds of millions of dollars.

A much more useful way to deal with the issue of disconnected numbers is for the FCC to adopt the NANC recommendation on Nationwide Number Portability. [6] If consumers did not have to disconnect their numbers when they moved out of rate centers and had to change providers then the disconnect problem would be substantially eliminated.

---

[6] http://www.nanc-chair.org/docs/mtg_docs/Aug16_ATIS_Report_National_Number_Portability_Attachment.pdf

The Commission should start with the least disruptive options for deployment and build on success *over time*. It is not necessary to consider every possible issue with the numbering plan or poorly allocated numbers at such a nascent stage of these activities.

Further action may be necessary to coordinate with the full North American Numbering Plan and its international partners to attempt to coordinate what numbers may or may not be included in the macro set of DNO numbers.

Blacklists & Whitelists

The most obvious issue the Commission must confront with these classes of databases is the issue of blacklists. The problem with blacklists is how do you get off one if you are inadvertently put on one. This is a scourge that often confronts individuals and businesses that own and manage their own Internet domains. I have had this problem with shockey.us for instance. I have personally been subjected to such inadvertent or malignant indignities to the point where I could not even receive email since my domain was blocked and the blacklist to which I was put on provided no input on how to get off. This kind of situation is unacceptable for the critical voice/text communications networks of the United States. The Commission must insist that there be some form of remediation procedure be adopted by the industry to prevent such occurrences.

In addition, it is becoming increasingly clear via anecdotal evidence that the robocall spoofing perpetrators have already begun to move their activities from the non-allocated or malformed NANP numbers directly to allocated parts of the NANP where more advanced Call Validation techniques such as STIR/SHAKEN and Call Validation Display to the consumers end devices will be necessary. [7] [8] The reason for this is obvious. The perpetrators

---

[7] https://finance.yahoo.com/news/spam-robocalls-increasing-whats-done-155053979.html

[8] http://www.cnbc.com/2017/06/25/robocalling-soars-despite-do-not-call-registry-as-scammers-couldnt-care-less-about-bothering-consumers.html

know if you see a NPANXX on your display relatively close to your home number there may be a perception that the call comes from a neighbor, relative or business that you have had a prior relationship with in the past. You answer the phone. [9]

This development does not argue that a Do Not Originate database is irrelevant only that there will have to be eternal vigilance in countermeasures to thwart the efforts of robocall spammers and that we do not create onerous requirements on the industry that may have already been overtaken by technology.

The Commission did not address the underlying business model by which such a DNO list would be established. That question may be under further consideration but it is clear that the existing model of the US Do Not Call list, managed by the Federal Trade Commission is a reasonable model to consider. [10] The structure of the list is relatively static. A master file is available for download and an update file can be made available on a daily or weekly basis. This would permit larger carriers to locally cache the DNO list in their network and smaller providers can subscribe to a third-party service if their staff is insufficiently large enough to manage the system locally. This model is well understood in Local Number Portability.

The question is then how should this DNO be funded? In my opinion, this list should be funded out of the general Congressional appropriation to the Federal Communications Commission and contracted out to an appropriate vendor under the well-established rules for such things. I do not recommend cost recovery mechanisms specific to the voice communications industry that would be collected through the normal FCC 499 forms. The voice communications industry has enough regulatory fees as it is.

---

[9] http://www.npr.org/2017/07/31/540515367/familiar-looking-numbers-are-the-latest-twist-in-robocalls

[10] https://www.donotcall.gov/faq/faqbusiness.aspx#accessTelNumbers

Call Authentication Trust Anchor and STIR/SHAKEN

The SIP Forum has undertaken a partnership with the Alliance for Telecommunications Industry Solutions [ATIS] to cooperate on developing technical standards to combat robocalls and spoofing. This partnership has been duly noted in the Industry Strikeforce reports. We have been working on these issues for many years now and we are not finished.

To review the accomplishments of the SIP Forum/ATIS NNI alliance so far.

In 2015 we completed a set of Specifications for Network to Network Interfaces [NNI] between SIP/IMS networks. [11]

In 2016 we completed a Recommendation on the architectural framework for STIR/SHAKEN. [12]

ATIS and the SIP Forum have recently completed a recommendation on a Certificate Management framework that would implement the STIR/SHAKEN protocols and establish National Trust Anchor for the US portions of the NANP. In this document, we foresee a critical role for the FCC.

1. Without reservation, I support the establishment of a United States Call Authentication Trust Anchor based on the joint ATIS SIP Forum work.
2. I support the active, critical and ongoing role the Federal Communications Commission will have in the establishment of this Trust Anchor. I agree with the Commission that it has all the Authority to Act it needs under Section 251 (e) 1 of the Act.
3. I support mandating STIR/SHAKEN within the United States, taking into consideration various industry participants will need time to implement and that we are still working

---

[11] https://www.sipforum.org/2015/07/atis-and-sip-forum-complete-new-ip-based-network-to-network-interface-nni-technical-specification/

[12] https://www.fcc.gov/ecfs/filing/10224016569773

our way through various issues in Technology Transitions from the PSTN SS7-TDM to all IP voice networks.

4. I support moving to a Notice of Proposed Rule Making on establishing the Trust Anchor at the earliest possible date.
5. I note that though the STIR/SHAKEN initially proposes a service provider to service provider Authentication model, this does not preclude *eventual* adoption of credentials pushed closes to the end user such as a IP-PBX or cloud UCaaS provider or the incorporation of requirements for various OTT vendors.
6. It is absolutely vital that the mandate include international wholesale providers where many of us believe the center of the problem lies. This traffic cannot be allowed into the United States unless the provider is capable of attesting to its origin at the international call gateway and having sufficient capability to permit both the Commission and Law Enforcement to Track and Trace the traffic.

Why mandate STIR/SHAKEN?

IMHO the system will not work unless it is mandated. I ask the Commission to consider the long often tortured history of Local Number Portability. The establishment of LNP was one the most successful regulatory interventions of the 1996 Act.

LNP worked. It worked better than many of us could possibly imagined. Not only did voice communications become more competitive and cheeper, it drove the adoption of more cost-effective technologies such as SIP into the network. In addition, the technical abstraction of network naming vs addressing ultimately simplified the voice network itself to the benefit of the industry as a whole.

LNP would have never worked if it was voluntary. It had to be mandated to ensure that the playing field was level for everyone. It was expensive, to be sure, but any rational cost-benefit analysis of the cost of LNP to the industry vs the billions and billions saved by American consumers and businesses should be self-evident.

2017 is not 1996. The United States Voice Communications system has its economic challenges, among them very thin margins and relatively flat revenue. Some companies are well positioned to implement STIR/SHAKEN with the Trust Anchor, others are not. If the burden is not equally shared a few consumers and enterprises will see the benefits and the rest will be left to suffer the ongoing plague of robocalls and caller ID spoofing. That is simply unacceptable.

There are some costs involved here. First is the cost to industry. For those operators with advanced SIP/IMS infrastructures the costs should be reasonable and well within normal software upgrade cycles. There are issues how classic TDM/SS7 networks will incorporate the technology but, standards bodies are working on some ideas right and in any event, we need to move away from TDM/SS7.

How long is this going to take? That question needs further comment in a NPRM but I would guestimate 3-5 years The Commission needs to understand how these requirements are incorporated into a real product or service.

a. Telecom carriers need to establish the requirements. That process is partially underway. A mandate forces the issue.
b. The telecom supplier community needs to code it. (at least a year).
c. Then the carriers need to test it well before it is deployed in the network. (6-8 months?) The industry is very very careful about Security Reliability and Interoperability issues for good reason. That takes time.
d. Of course, in the meantime the Commission would actually have to establish the Trust Anchor…well we all know how long that might take. Again, looking at the LNP history offers some reasonable picture of how this would deploy.

The operation of the Trust Anchor itself to the FCC IMHO should not exceed 20 Million per year inclusive of startup costs. The Commission has several funding options at its disposal including the NANPA and NAPM models.

I do not support incorporation of the Call Authentication Trust Anchor into either the NANPA or NAPM administrations. STIR/SHAKEN is a separate type of type of technology that will require a different types of skill sets. A third option is recommended.

In any event there is extremely important role for the North American Numbering Council in assisting the Commission in coordinating implementation activities. As a current member of the NANC, I am well acquainted with the excellent work they do. In addition, I recommend the Commission seek the guidance of National Institute of Standards and Technology [NIST] for technical recommendations on the STIR/SHAKEN Public Key Infrastructure proposals. NIST has a long and distinguished technical background in these matters.

Call Display Framework

ATIS and the SIP Forum is currently undertaking a work plan to define a Call Validation Display Framework which addresses the ultimate issue of how Call Validation data from the STIR/SHAKEN can be delivered directly to consumers phones or other User Agents to permit them to make informed decisions on if or how they may wish to receive calls. In my humble opinion, this is the keystone to robocall spoofing remediation. We must empower consumers, and enterprises in this process. This will be complicated. Many us looking at this proposal are Network Engineers and do not have a background in User Interface Design principals. The industry as a whole will need careful and reasoned input from the Federal Communications Commission, the Federal Trade Commission and other interested parties as it develops its recommendations.

There are issues of what data should be displayed to the consumer, why and for what purpose. The consumer may only have 2-3 seconds to make a decision on whether to answer a call or not. Should visual elements accompany Call Validation Data on the phone or user device such as green, yellow or red symbols? What text is needed? Which network data elements should be considered objective vs subjective data? The needs of consumers may be very different from data needed by enterprises. It is increasingly clear that STIR/SHAKEN may have immense value to enterprises that need to quickly contact consumers about various

transactions that affect their daily lives. The Financial Services industry needs to alert consumers if there are potential fraud activity in their accounts. The Health Care industry certainly needs to contact consumers to inform them of potential issues regarding their health, such as test results. The Utility industry has another set of vital public safety needs. Last but not least there are potentially vast National Security / Emergency Preparedness [NS/EP] applications where the Call Display Framework could be useful.

Conclusion

The Commission should consider measured, tailored and especially realistic proposals that do not over burden the industry as it implements these proposals. Build from success, then expand the scope of these proposals as the evidence suggests. We are rebuilding trust in the system. This will take time. We should be building "Rings of Defense" beginning with those technologies that are relatively easy to implement first.

1. The Commission should adopt the Do Not Originate proposal that only includes relatively static number elements and do not include reassigned numbers*, at this time.* It's clear that attempting to impose a burden of real-time database access on providers may incur costs that could better be used to implement more promising technologies in the short term and network upgrades in general.

2. The Commission should adopt and mandate the STIR/SHAKEN framework noting various industry participants may need extra time to implement. Reviewing the history of Local Number Portability may be a useful historical guide. 3-5 years seems reasonable.

   I'm at the disposal of the Commission and staff if there are any further questions. I would also be interested is discussions with various industry participants outside the telecommunications that have an interest in these proposals. Specifically, those industry associations working in Financial Services, Health Care and Utilities.

Respectfully submitted,

Richard Shockey
Shockey Consulting
2427 Silver Fox Lane
Reston, Virginia 20191
Voice +1 703 593 2683
E Mail richard@shockey.us

August 14, 2017